

#2
1-25-02
PATENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Boris GEFWERT

Serial No. (unknown)

Filed herewith

METHOD AND ARRANGEMENT FOR
MANAGING DATA TRANSMISSION
IN A DATA NETWORK



**CLAIM FOR FOREIGN PRIORITY UNDER 35 U.S.C. 119
AND SUBMISSION OF PRIORITY DOCUMENT**

Assistant Commissioner for Patents

Washington, D.C. 20231

Sir:

Attached hereto is a certified copy of applicant's corresponding patent application filed in Finland on July 21, 2000, under No. 20001700.

Applicant herewith claims the benefit of the priority filing date of the above-identified application for the above-entitled U.S. application under the provisions of 35 U.S.C. 119.

Respectfully submitted,

YOUNG & THOMPSON

By

Benoît Castel

Benoît Castel
Attorney for Applicant
Registration No. 35,041
Customer No. 00466
745 South 23rd Street
Arlington, VA 22202
Telephone: 703/521-2297

July 23, 2001

Helsinki 1.6.2001

ETUOIKEUSTODISTUS
PRIORITY DOCUMENT

J1040 U.S. PTO
09/909883
07/23/01



Hakija
Applicant

Suomen Posti Oy
Helsinki

Patenttihakemus nro
Patent application no

20001700

Tekemispäivä
Filing date

21.07.2000

Kansainvälinen luokka
International class

H04L

Keksinnön nimitys
Title of invention

"Menetelmä ja laitteisto tiedonsiirron hallitsemiseksi tietoverkossa"

Täten todistetaan, että oheiset asiakirjat ovat tarkkoja jäljennöksiä patentti- ja rekisterihallitukselle alkuaan annetuista selityksestä, patenttivaatimuksista, tiivistelmästä ja piirustuksista.

This is to certify that the annexed documents are true copies of the description, claims, abstract and drawings originally filed with the Finnish Patent Office.


Pirjo Kaila
Tutkimussihteeri

Maksu 300,- mk
Fee 300,- FIM

Osoite: Arkadiankatu 6 A Puhelin: 09 6939 500 Telefax: 09 6939 5328
P.O.Box 1160 Telephone: + 358 9 6939 500 Telefax: + 358 9 6939 5328
FIN-00101 Helsinki, FINLAND

Menetelmä ja laitteisto tiedonsiirron hallitsemiseksi tietoverkossa - Förfarande och anordning för att behärska dataöverföring i ett datanät

Keksinnön kohteena on menetelmä ja laitteisto tiedonsiirron hallitsemiseksi tietoverkossa. Erityisesti keksintö koskee luottamuksellisen tiedon välittämistä tietoverkossa.

- 5 Tietoverkkojen ja erityisesti Internet-tietoverkon käyttö on lisääntynyt nopeasti. Tietoverkoissa tuotetaan, jaetaan, myydään ja kulutetaan informaatiota ja palveluja erilaisissa muodoissa. Eräänä palveluna mainittakoon esimerkiksi erilaiset tietoverkkolehdet, jotka tuotetaan ja kulutetaan verkkoympäristössä. Vastaavasti erilaisia asiakirjoja, sekä julkisia että salaisia ja henkilökohtaisia asiakirjoja käsitellään tietoverkossa. Tämän vuoksi, vaikka esim. Internet on julkinen tietoverkko, se sisältää
- 10 lukuisia palvelimia, joiden tiedostoihin pääsy on rajoitettu vain tietyille käyttäjille.

- Tietoverkko on väline, jonka kautta informaatiota siirretään lähteestä yhteen tai useampaan kohteeseen sähköisinä (tai optisinä) signaaleina edullisimmin digitaalisessa muodossa peräkkäin lähetettävänä yksikköinä eli tietopaketteina. Pakettipohjaiset
- 15 verkot ja niissä käytettyjen pakettien ja kehysten rakenne on standardoitu. Pakettiin kuuluu joukko kenttiä, joissa digitaalisessa muodossa bitteinä esitetään erilaista yhteyden solmimisen ja ylläpitämisen kannalta merkityksellistä tietoa, kuten vastaanottajan (kohde) ja lähettäjän (lähde) osoitetiedot, varsinaisen vastaanottajalle tarkoitetun informaation lisäksi. Kun tietopakettia käsitellään verkon solmukohdissa ja lopullisessa määränpäässä, tarkistetaan, onko tietopaketti virheetön ja vastaanottaja
- 20 oikea, suoritetaan mahdollisesti kuittaus lähettäjälle ja virhetilanteessa pyydetään lähettämään sama tietopaketti uudelleen. Tietopaketin arviointi toteutetaan sen eri kenttien sisältämien tietojen perusteella.

- Internet on julkinen tietoverkko, jonka kautta välitetään informaatiota pakettimuodossa TCP/IP (Transmission Control Protocol / Internet Protocol) -protokollaperheessä määritetyllä tavalla. Ongelmana Internetissä on luottamuksellisten ja/tai maksullisten tietojen ja palvelujen välittäminen, koska ilman erityisiä toimenpiteitä
- 25 kenen tahansa on mahdollista päästä käsiksi verkkoon kytkettyihin tietokantoihin.

- Tunnetaan keinoja Internetin ja vastaavien julkisten verkkojen tietoturvallisuuden parantamiseksi. Yhteyden salaamiseen lähettäjältä vastaanottajalle on käytettävissä salausohjelmia, joiden avulla lähetettävät tietopaketit salakirjoitetaan määrättyllä tavalla ja vastaavasti vastaanotettavien tietopakettien salakirjoitus puretaan. Ylei-
- 30

simmin käytetään ns. julkiseen avaimeen perustuvia salausmenetelmiä. Yksittäisten yhteyksien kohdalla tämä on varsin toimiva ratkaisu, mutta kun vastaanottajien ja lähettäjien sekä yhteyksien määrä ja nopeus kasvavat suureksi, muodostuu ongelmia. Luvaton pääsy verkkoon kytkettyyn tietokoneeseen tai tiettyyn tietolähteeseen/palveluun estetään tunnuksen, salasanan tai vastaavan avulla.

5 Tekniikan tason mukaisiin järjestelyihin liittyy kuitenkin eräitä epäkohtia. Jos käyttäjä käyttää esim. Internetissä useita palveluja, joihin tarvitaan rekisteröityminen, hänen tulee muistaa useita salausavaimia ja käyttäjätunnuksia. Koska tällaisia tunnuksia on vaikea muistaa ulkoa, niistä usein tehdään luettelo, jonka mukana kuljet-

10 taminen on hankalaa ja joka voi joutua asiaankuulumattomien tahojen käyttöön. Tunnukset voivat joutua asiaankuulumattomien käyttöön myös siten, että tietoverkon tietoliikennettä seurataan, tai että käyttäjä tahallisesti levittää maksullisen palvelun käyttäjätunnuksiaan lähipiirilleen, jolloin palvelun tuottajalta jää osa käytettyjen palvelujen tuotoista saamatta.

15 Edellä mainittuja tunnusten väärinkäyttöön liittyviä ongelmia on pyritty korjaamaan siten, että tunnuksia vaihdetaan säännöllisin väliajoin tai aina palvelua käytettäessä. Tällöin käyttäjä joutuu kuitenkin käyttämään vielä suurempaa määrää tunnuksia, mikä tekee palveluiden käytön hankalaksi.

Lisäksi tekniikan tason mukaisten ratkaisujen puutteena on, että mikäli henkilölle tulisi antaa esim. virallinen tiedote verkkoympäristössä, ei olisi selvää, mihin se tulisi toimittaa, millä tavoin, ja mitkä ovat siirtoon osallistuvien osapuolten vastuut viestin perilletulon varmistamiseksi. Virallisia tiedotteita voivat olla esim. tiedote

20 äänioikeudesta, haaste oikeuteen tms.

Keksinnön tarkoituksena on luoda ratkaisu tiedonsiirron hallitsemiseksi, jonka avulla edellä mainittuja, tekniikan tasoon liittyviä epäkohtia voidaan vähentää. Esillä oleva keksintö pyrkii ratkaisemaan sen, kuinka tietoverkossa oleva informaatio/palvelu, joka on tarkoitettu tietylle kohteelle tai kohdejoukolle, osoitetaan näille ja kuinka tarvittavat oikeudet sen käyttöön annetaan. Lisäksi pyritään ratkaisemaan, kuinka verkossa tarvittavat informaation osoitteet ja käyttöoikeudet tuotetaan, jae-

25 taan, säilytetään, siirretään ja käytetään.

30

Keksinnön eräänä ajatuksena on se, että kun käyttäjälle tarkoitettu tieto on tallennettu, tallennuspaikan osoite siirretään käyttäjälle luotettavan tahon (välittäjän) välittämänä. Tällöin välittäjän suorittaman käyttäjän tunnistuksen perusteella käyttäjän on

mahdollista saada käyttöönsä useiden palvelun ja tiedon tuottajien/lähetäjien tiedot/palvelut.

Keksinnön mukaiselle menetelmälle tiedonsiirron hallitsemiseksi tietoverkossa on tunnusomaista, että menetelmä käsittää vaiheet, joissa

- 5 - tallennetaan määrätty tieto määrätyn osoitteen mukaiseen tallennuspaikkaan,
- siirretään välittäjälle osoitetieto, joka määrittelee määrätyn osoitteen,
- siirretään välittäjälle tieto ainakin yhdestä käyttäjästä, jolla on oikeus saada käyttöönsä mainittu määrätty tieto,
- tallennetaan mainittu osoitetieto välittäjän käyttäjäkohtaiseen hakemistoon, johon mainitulla ainakin yhdellä käyttäjällä on pääsy, ja
- 10 - siirretään mainittu määrätty tieto käyttäjälle mainitun osoitetiedon perusteella.

Keksinnön mukaiselle järjestelylle tiedonsiirron hallitsemiseksi tietoverkossa on tunnusomaista, että järjestely käsittää

- 15 - välineet määrätyn tiedon tallentamiseksi määrätyn osoitteen mukaiseen tallennuspaikkaan,
- välineet osoitetiedon siirtämiseksi välittäjälle, joka osoitetieto määrittelee määrätyn osoitteen,
- välineet siirtää välittäjälle tieto ainakin yhdestä käyttäjästä, jolla on oikeus saada käyttöönsä mainittu määrätty tieto,
- 20 - välineet tallentaa mainittu osoitetieto välittäjän käyttäjäkohtaiseen hakemistoon, johon mainitulla ainakin yhdellä käyttäjällä on pääsy, ja
- välineet siirtää mainittu määrätty tieto käyttäjälle mainitun osoitetiedon perusteella.

Keksinnön eräitä edullisia suoritusmuotoja on esitetty epäitsenäisissä patenttivaatimuksissa.

- 25
- 30 Keksinnön avulla saavutetaan huomattavia etuja tekniikan tason ratkaisuihin verrattuna. Käyttäjä voi käyttää useita tietoverkon palveluja ja tarvitsee kuitenkin vain yhden tunnistusmenettelyn saadakseen yhteyden välittäjän tiedostoon. Lisäksi keksinnön avulla tiedon/palvelujen tuottajat eivät tarvitse lainkaan käyttäjäkohtaisia tunnistus/salausmenettelyjä, koska kaikki tiedonsiirto voidaan suorittaa välittäjän ja palvelun tuottajan välisen, luotettavan yhteyden välityksellä, ja välittäjä on vastuussa kunkin käyttäjän tunnistamisesta ja tiedon salauksesta. Lisäksi tuottaja voi käyttää omia asiakasrekisterin käyttäjätunnuksia, eikä tuottajan tarvitse luoda käyttäjiä varten tarvitse omia tunnuksia tiedonsiirtomenettelyä varten.

Lisäksi keksinnön avulla on mahdollista saada aikaan luotettava varmiste lähetetyn tiedon vastaanottamisesta, koska tiedon välitys tapahtuu ulkopuolisen, luotettavan välittäjän toimesta. Siten tietoverkkoa voidaan käyttää myös sellaisen, esim. viranomaisen lähettämän tiedon välitykseen, jossa tiedon lähettäjän on saatava varmiste tiedon perille saapumisesta.

Tässä patenttihakemuksessa käytetään mm. seuraavia käsitteitä:

- "Tuottaja" on taho, kuten henkilö, yritys yhteisö, julkishallinto tai viranomainen, joka tarjoaa kohdennettua informaatiota tai palvelua verkossa.
- "Kuluttaja" on asiakas, henkilö, yritys yhteisö, julkishallinto tai viranomainen, joka käyttää hänelle kohdennettua informaatiota tai palvelua.
- "Välittäjä" on kolmas luotettava osapuoli, joka yhdistää ts. informaation tai palvelun sijainnin sekä siihen liitetyn käyttöoikeuden luotettavasti ja kiistämättömästi.
- "Palvelu" tai "määrätty tieto" on tietoverkossa olevaa tietosisältöä, kuten esim. asiakirja, tiliote, julkaisu tai muu palvelu, joka on saatavilla tietoverkosta tuottajan toimesta.
- "Osoite" määrittelee, missä verkon tietokoneessa/tiedostossa informaatio tai palvelu sijaitsee.
- "Oikeus" on tuottajan tuottama tunniste, jonka perusteella tuottaja tunnistaa, että käyttäjällä on oikeus palveluun.
- "Käyttöoikeus" sisältää käyttäjän tunnisteen, palvelun osoitteen ja oikeuden.
- "Allekirjoitus" on teknologia, jolla todennetaan viestin lähettäjä.
- "Salaus" on menettely, jolla salataan tietoverkossa lähetettävä viesti esim. julkisen avaimen menetelmällä.
- "Välityshakemisto" on välittäjän ylläpitämä käyttäjäkohtaisten osoitteiden ja käyttöoikeuksien säilytyspaikka, joka on käyttäjän käytettävissä.
- "Laatikosto" on välityshakemisto, joka on käytettävissä käyttäjän (kevyen) todentamisen perusteella.
- "Kassakaappi" välityshakemisto, joka on käytettävissä käyttäjän vahvan tunnistuksen perusteella.

Tarkastellaan ensimmäisenä esimerkkinä arkaluontoisen asiakirjan lähettämistä käyttäjälle. Asiakirjan tuottaja salakirjoittaa käyttäjän julkisella avaimella asiakirjan osoitteen. Tällöin ainoastaan käyttäjä voi saada tietoonsa, missä asiakirja sijaitsee. Tämän lisäksi tuottaja salakirjoittaa välittäjän julkisella avaimella käyttäjän tunnisteen. Tällöin ainoastaan välittäjä voi saada tietoonsa, kenelle käyttäjälle salakirjoitettu osoite on tarkoitettu. Tuottaja lähettää näin muodostetun käyttöoikeusviestin välittäjälle. Näin salataan ulkopuolisilta sekä käyttäjä että osoite. Välittäjä avaa viestin omalla tunnuksellaan sekä tunnistaa viestistä käyttäjän. Tämän jälkeen välittäjä sijoittaa linkin käyttäjän välityshakemistoon, esim. kassakaappiin. Välittäjä ei pysty avaamaan salakirjoitettua osoitetta.

Käyttäjä avaa kassakaappinsa omalla tunnuksellaan ja hakee kassakaappiin tallennetun linkin avulla asiakirjan käyttöönsä. Tuottajan ei siten tarvitse erikseen lähettää asiakirjaa. Linkissä on tarvittaessa määritelty myös itse asiakirjan sisällön siirron salausrmekanismi.

Oletetaan, että välitettävä asiakirja on tietylle käyttäjälle kohdistettu virallinen tiedote, kuten esim. haaste alioikeuteen tai ilmoitus äänioikeudesta. Tällöinkin toimitaan pääsääntöisesti, kuten edellä on kuvattu. Tämän lisäksi välittäjä voi informoida viranomaista (tuottajaa), että viesti on vastaanotettu, että viesti on sijoitettu kuluttajan saataville kassakaappiin, että kuluttaja on käynyt kassakaapillaan taio että kuluttaja on käyttänyt käyttöoikeutta jne.

Seuraavaksi tarkastellaan esim. maksullisten palvelujen välittämistä. Sisällöntuottaja (tuottaja), julkaistessaan esim. uuden verkkolehden, muodostaa tilaajilleen (käyttäjille) numerokohtaisen käyttöoikeuden ja lähettää sen käyttöoikeusviestinä välittäjälle. Välittäjä sijoittaa käyttöoikeusviestin sisältämän osoitetiedon käyttäjän välityshakemistoon, esim. laatikostoon. Käyttäjä avaa laatikoston ja huomaa, että uusi lehti on julkaistu ja voi ottaa sen käyttöönsä osoitetiedon avulla.

Kauppia ja logististen palvelujen tuottaja voi lähettää lähetyskohtaisen tunnisteen (käyttöoikeusviestin) välittäjälle, joka sijoittaa sen ostajan (käyttäjän) välityshakemistoon, kuten laatikostoon, ja informoi tästä ostotilanteesta. Ostajan ei tarvitse muistaa erillisiä tunnisteita vaan voi aktivoida lähetyksen statustilanteen omasta laatikostaan.

Kanta-asiakkuuden antaja (tuottaja) voi muodostaa käyttöoikeuden kanta-asiakkaan ajankohtaiseen tiliotteeseen (käyttäjä) ja lähettää käyttöoikeusviestin välittäjälle, joka sijoittaa sen käyttäjän välityshakemistoon, kuten esim. laatikostoon. Käyttäjä voi

6

seurata kaikkea kanta-asiakkuusinformaatiotaan ilman yrityskohtaisia tunnuksia ja salasanoja.

Käyttäjä voi myös siirtää esim. hallintaan perustuvan oikeuden toiselle käyttäjälle lähettämällä käyttöoikeusviestin välittäjälle, joka sijoittaa käyttöoikeuden uuden
5 käyttäjän välityshakemistoon, kuten esim. laatikostoon.

Oikeus voi ylipäättään olla esim. henkilökohtainen, yrityskohtainen, hallintaan perustuva tai aikaan, tapahtumamäärään tai rahalliseen arvoon sidottu.

Seuraavassa keksintöä selostetaan viitaten oheisiin piirustuksiin, joissa

- 10 kuva 1 esittää vuokaaviota eräästä keksinnön mukaisesta menetelmästä käyttöoikeuden muodostamiseksi,
- kuva 2 esittää vuokaaviota eräästä keksinnön mukaisesta menetelmästä käyttöoikeuden välittämiseksi,
- kuva 3 esittää vuokaaviota eräästä keksinnön mukaisesta menetelmästä käyttöoikeuden käyttämiseksi,
- 15 kuva 4 esittää lohkoakaaviota eräästä keksinnön mukaisesta järjestelystä tiedon välittämiseksi, ja
- kuva 5 esittää erästä keksinnön mukaista käyttäjäkohtaista välityshakemistoa, jossa osoitetiedot esiintyvät linkkeinä.

20 Kuva 1 esittää vuokaaviota eräästä keksinnön mukaisesta menetelmästä käyttöoikeuden muodostamiseksi 100. Tässä esimerkissä tarkastellaan asiakirjan käyttöoikeuden muodostamista. Kun tuottaja on tuottanut asiakirjan, se määrittelee hakuosoitteen, 105, josta ko. asiakirja on haettavissa. Hakuosoite voi olla käyttäjäkohtainen tai se voi olla yhteinen usealle käyttäjälle. Asiakirja tallennetaan siten, että se on haettavissa tietoverkosta määritetyn osoitteen avulla, 110.

25 Tämän jälkeen määritetään yksi tai useampi käyttäjä, jolla on oikeus saada asiakirja käyttöönsä, 115. Määritetty osoite ja asiakirjan nimi muodostetaan osoitelinkiksi ja salataan ko. käyttäjän julkisella avaimella, 120, siten, että salaus on vain käyttäjän purettavissa. Tämän jälkeen muodostetaan käyttöoikeusviesti siten, että käyttäjän tunnistetiedot ja salattu, määritetty osoite salataan edelleen välittäjän julkisella avaimella,
30 125, jolloin ainoastaan välittäjä voi saada tietoonsa käyttäjän tunnisteen käyttöoikeusviestistä. Lopuksi muodostettu käyttöoikeusviesti siirretään tuottajalta välittäjälle,

128. Jos usealla käyttäjällä on käyttöoikeus ko. asiakirjaan, tuottaja muodostaa jo-
kaista käyttäjää vastaavan käyttöoikeusviestin, ja lähettää ne välittäjälle.

5 Kuva 2 esittää vuokaaviota eräästä keksinnön mukaisesta menetelmästä käyttöoi-
keuden välittämiseksi, 200. Kun välittäjä on vastaanottanut salatun käyttöoikeus-
viestin, 230, se purkaa käyttöoikeusviestin ensimmäisen salauksen välittäjän tun-
nuksella, 235. Välittäjä voi tämän jälkeen lukea puretusta viestistä käyttäjätunnuk-
sen, 240. Välittäjällä on luettelo tuottajan käyttämistä käyttäjätunnuksista ja niitä
10 vastaavista käyttäjistä. Tämän luettelon perusteella välittäjä määrittää vastaanotetun
viestin sisältämää käyttäjätunnusta vastaavan käyttäjän, 245. Kun käyttäjä on määri-
tetty, käyttöoikeusviestin sisältämä salattu osoitetieto tallennetaan käyttäjän välitys-
hakemistoon osoitelinkiksi, 250. Näin käsitellään kaikki vastaanotetetut käyttöoike-
usviestit.

15 Kuva 3 esittää vuokaaviota eräästä keksinnön mukaisesta menetelmästä käyttöoi-
keuden käyttämiseksi, 300. Kun käyttäjä haluaa tarkistaa hänelle saapuneet käyttö-
oikeudet, hän ottaa yhteyden välittäjään tietoverkon välityksellä, 360. Käyttäjä pys-
tyy avaamaan hänen henkilökohtaisen välityshakemistonsa omalla tunnuksellaan,
365, jolla välityshakemiston sisältämien osoitelinkkien salaus puretaan. Tällöin väli-
tyshakemistoon tallennettujen osoitelinkkien nimet ovat käyttäjän luettavissa. Käyt-
tämä valitsee tämän jälkeen sen osoitelinkin, johon liittyvän asiakirjan (tai muun pal-
20 velun) hän haluaa hakea käyttöönsä, 370. Käyttäjä aktivoi valitun osoitelinkin, 375,
minkä jälkeen järjestelmä hakee tietoverkosta ko. linkin sisältämän osoitteen perus-
teella valitun asiakirjan käyttäjän käyttöön, 380.

25 Jotta käyttäjä pääsee lukemaan välityshakemistonsa, välittäjä voi edellyttää käyttäjän
tunnistusmenettelyn. Tämä tunnistusmenettely voi olla sitä vahvempi, mitä suurem-
paa luottamuksellisuutta halutaan. Käyttäjällä voi myös olla useampia välityshake-
mistoja, jolloin eri välityshakemistoihin pääsy edellyttää eri vahvuista tunnistusme-
nettelyä. Tunnistusmenettelyltä edellytettävä vahvuus voidaan ilmaista käyttöoike-
usviestissä käyttäjätunnisteen yhteydessä, jolloin välittäjä tallentaa käyttöoikeuden
sellaiseen käyttäjän välityshakemistoon, johon pääsy edellyttää riittävän vahvan
30 käyttäjätunnistuksen.

Jos luottamuksellisen asiakirjan yhteydessä halutaan varmistaa, että käyttäjä on saa-
nut/käyttänyt asiakirjan tämä voidaan suorittaa esim. seuraavasti. Kun käyttäjä pyy-
tää välityshakemistostaan ao. asiakirjan avaamista, välittäjä rekisteröi pyynnön. Nyt
myös itse asiakirja välitetään käyttäjälle välittäjän toimesta, jolloin välittäjä voi re-
35 kisteröidä myös sen, että käyttäjä on vastaanottanut asiakirjan. Tällaisessa asiakir-

- jassa on edullisesti salauksen purkuun liittyvä tunniste, jonka välittäjä lähettää tuottajalle, joka edelleen rekisteröi tapahtuman. Tuottaja toimittaa tunnisteiden mukaisen salauksenpurkuavaimen välittäjälle, joka puolestaan toimittaa sen käyttäjälle. Näin voidaan varmistua siitä, että käyttäjä on saanut asiakirjan ja halunnut purkaa sen salauksen. Mikäli esim. tietoliikenneyhteys katkeaisi niin, että käyttäjä ei saa salauksenpurkuavainta, se voidaan pyytää uudestaan. Käyttäjän päätteessä on edullisesti ohjelmisto, joka voi latautua välittäjän palvelimelta esim. ensimmäisen pyynnön yhteydessä ja joka lähettää automaattisesti välittäjälle kuittauksen salauksenpurkuavaimen saannista.
- 5
- 10 Verkkopalvelujen yhteydessä saattaa olla tarpeellista estää saman käyttäjälinkin rinnakkainen käyttö usean käyttäjän toimesta. Tämä voidaan estää esim. siten, että todellinen linkki tuottajan palveluun on välittäjän hallussa. Palvelun ensimmäinen käyttöönotto tapahtuu näin aina välittäjän palvelimen kautta, jolloin tunnistetaan sekä käyttäjä että päätelaite, jolta palvelupyyntö saadaan. Pyyntö välitetään tuottajalle
- 15 lisättynä lisätiedoilla, kuten käyttäjän ja päätelaitteen tunnisteet, mahdollinen aika-leima jne. Tämä tekee mahdolliseksi luvallisen käyttäjän tunnistamisen ja ns. väliaikaisserтификаatin myöntämisen. Nämä tiedot salakirjoitetaan avainparilla, jotka ovat välittäjän ja tuottajan tiedossa, ja siirretään tuottajalle. Eräs vaihtoehtoinen ratkaisu olisi se, että kaikki palvelupyynnot käyttäjän ja tuottajan välillä välittyvät välittäjän
- 20 kautta, jolloin voidaan aina todentaa käyttöoikeuden olemassaolo.
- Kuva 4 esittää lohkokaaaviota eräästä keksinnön mukaisesta järjestelystä tiedon välittämiseksi. Järjestely käsittää Internet-tietoverkkoon 430 liitynyt tuottajan laitteiston 410, käyttäjän laitteiston 420 sekä välittäjän laitteiston 440. Tuottajan laitteisto 410 käsittää tuottajan palvelimen 411, joka on liitetty Internet-tietoverkkoon. Tuottajan palvelimeen liittyy tietokanta 413, johon tallennetaan käyttäjien haettavissa olevat asiakirjat, tietopalvelut jne. Lisäksi tuottajan laitteistoon kuuluu rekisteri 412, joka käsittää tiedot tuottajan asiakkaista/käyttäjistä. Näihin käyttäjätietoihin kuuluvat tuottajan käyttämät asiakastunnisteet eli käyttäjätunnisteet sekä käyttäjien julkiset avaimet. Näiden tietojen avulla tuottajan palvelin muodostaa välittäjälle toimitettavat käyttöoikeusviestit.
- 25
- 30 Välittäjän laitteistoon 440 kuuluu välittäjän palvelin 441, joka on liitetty Internet-tietoverkkoon. Välittäjän palvelimeen liittyy tietokanta 448, johon tallennetaan käyttäjäkohtaiset välityshakemistot. Lisäksi välittäjän palvelimeen liittyy käyttäjärekisterit 446, joissa on tarvittavat tiedot käyttäjistä ja käyttäjien tunnistusmenetlyistä, joilla käyttäjä tunnistetaan tämän pääsemiseksi yhteen tai useampaan käyttäjäkohtaiseen välityshakemistoon. Lisäksi välittäjän palvelimeen liittyvät tuottajare-
- 35

2

kisterit, joissa on tiedot eri tuottajien kanssa käytettävästä mahdollisesta tiedonsiirron salausmenettelystä sekä luettelot tuottajien käyttämistä käyttäjätunnisteista sekä niiden vastaavuudesta välittäjän käyttäjärekisterissä oleviin käyttäjiin.

5 Käyttäjän päätelaite 420 voi olla tavanomainen Internet-tietoverkkoon esim. modemin avulla liitetty tietokone, jossa on tarvittavat selainohjelmat ja mahdolliset tiedonsiirron salausohjelmat.

10 Kuva 5 esittää erästä välittäjän ylläpitämää välityshakemistoa sellaisena, kun se avautuu käyttäjän päätteelle, 50. Välityshakemistossa on esitetty välittäjän nimi 51 ja käyttäjän nimi 52. Tiedot saapuneista linkkiosoitteista on esitetty riveinä samaan tapaan kuin tunnetuissa sähköpostihakemistoissa. Saapuneista linkeistä on omissa sarakkeissaan esitetty lähettäjä, aihe, linkki ja lähetyksen päivämäärä. Saapuneen tiedoston avaaminen tapahtuu aktivoimalla haluttu linkki. Itse linkkiosoitetta ei tarvitse esittää käyttäjän hakemistossa, vaan tiedosto voidaan avata esim. aktivoimalla halutun linkin ”aihe”, jolloin tiedosto haetaan tallennetun linkkiosoitteen perusteella.

15

Edellä on esitetty vain eräitä keksinnön mukaisen ratkaisun suoritusmuotoja. Keksinnön mukaista periaatetta voidaan luonnollisesti muunnella patenttivaatimusten määrittelemän suoja-alueen puitteissa esim. toteutuksen yksityiskohtien sekä käyttöalueiden osalta.

Patenttivaatimukset

1. Menetelmä tiedonsiirron hallitsemiseksi tietoverkossa, **tunnettu** siitä, että menetelmä käsittää vaiheet, joissa
 - tallennetaan määrätty tieto määrätyn osoitteen mukaiseen tallennuspaikkaan (105, 110),
 - siirretään välittäjälle osoitetieto, joka määrittelee määrätyn osoitteen (128),
 - siirretään välittäjälle tieto ainakin yhdestä käyttäjästä, jolla on oikeus saada käyttöönsä mainittu määrätty tieto (115),
 - tallennetaan mainittu osoitetieto välittäjän käyttäjäkohtaiseen välityshakemistoon, johon mainitulla ainakin yhdellä käyttäjällä on pääsy (250), ja
 - siirretään mainittu määrätty tieto käyttäjälle mainitun osoitetiedon perusteella (380).
2. Patenttivaatimuksen 1 mukainen menetelmä, **tunnettu** siitä, että mainittu osoitetieto salataan käyttäjän julkisella avaimella, jolloin osoitetiedon salaus on käyttäjän purettavissa (120, 365).
3. Patenttivaatimuksen 1 mukainen menetelmä, **tunnettu** siitä, että mainittu käyttäjätieto salataan välittäjän julkisella avaimella (125), jolloin välittäjä purkaa käyttäjätiedon salauksen tallentaa osoitetiedon käyttäjäkohtaiseen välityshakemistoon mainitun käyttäjätiedon perusteella (235-250).
4. Patenttivaatimuksen 1 mukainen menetelmä, **tunnettu** siitä, että käyttäjän ja ensimmäisen välityshakemiston välille muodostetaan yhteys käyttäjän tunnistuksen perusteella.
5. Patenttivaatimuksen 4 mukainen menetelmä, **tunnettu** siitä, että yhtä käyttäjää varten muodostetaan kaksi välityshakemistoa, jolloin käyttäjän ja ensimmäisen välityshakemiston välille muodostetaan yhteys käyttäjän ensimmäisen tunnistuksen perusteella ja käyttäjän ja toisen välityshakemiston välille muodostetaan yhteys käyttäjän toisen tunnistuksen perusteella, jolloin ensimmäinen ja toinen tunnistus poikkeavat toisistaan tunnistukselle ominaisen luotettavuuden (vahvuuden) perusteella.
6. Patenttivaatimuksen 1 mukainen menetelmä, **tunnettu** siitä, että välittäjä välittää määrätyn tiedon käyttäjälle.
7. Patenttivaatimuksen 6 mukainen menetelmä, **tunnettu** siitä, että
 - käyttäjä esittää välittäjälle pyynnön määrätyn tiedon vastaanottamiseksi,
 - käyttäjälle toimitetaan salauksenpurkuavain määrätyn tiedon salauksen pur-

kamiseksi,

- salauksenpurkuavaimen toimittaminen käyttäjälle rekisteröidään osoituksena asiakirjan vastaanottamisesta.

5 8. Järjestely tiedonsiirron hallitsemiseksi tietoverkossa, **tunnettu** siitä, että järjestely käsittää

- välineet määrätyn tiedon tallentamiseksi määrätyn osoitteen mukaiseen tallennuspaikkaan (411, 413),

- välineet osoitetiedon siirtämiseksi välittäjälle, joka osoitetieto määrittelee määrätyn osoitteen (411, 430, 441),

10 - välineet siirtää välittäjälle tieto ainakin yhdestä käyttäjästä, jolla on oikeus saada käyttöönsä mainittu määrätty tieto (411, 412, 430, 44),

- välineet tallentaa mainittu osoitetieto välittäjän käyttäjäkohtaiseen hakemistoon, johon mainitulla ainakin yhdellä käyttäjällä on pääsy (441, 448), ja

15 - välineet siirtää mainittu määrätty tieto käyttäjälle mainitun osoitetiedon perusteella (413, 411, 430, 420).

9. Patenttivaatimuksen 8 mukainen järjestely, **tunnettu** siitä, että se käsittää lisäksi välineet mainitun osoitetiedon salaamiseksi käyttäjän julkisella avaimella, jolloin osoitetiedon salaus on käyttäjän purettavissa (411, 412).

20 10. Patenttivaatimuksen 8 mukainen järjestely, **tunnettu** siitä, että se käsittää lisäksi välineet mainitun käyttäjätiedon salaamiseksi välittäjän julkisella avaimella ennen siirtoa välittäjälle, välineet käyttäjätiedon salauksen purkamiseksi välittäjälle siirron jälkeen ja välineet osoitetiedon tallentamiseksi käyttäjäkohtaiseen välityshakemistoon mainitun käyttäjätiedon perusteella (411).

25 11. Patenttivaatimuksen 8 mukainen järjestely, **tunnettu** siitä, että se käsittää välineet käyttäjän tunnistamiseksi käyttäjän ja välittäjän välisen yhteyden muodostamiseksi (441, 446).

30 12. Patenttivaatimuksen 11 mukainen menetelmä, **tunnettu** siitä, että se käsittää välineet kahden välityshakemiston muodostamiseksi yhtä käyttäjää varten, yhtä käyttäjää varten muodostetaan kaksi välityshakemistoa, välineet yhteyden muodostamiseksi käyttäjän ja ensimmäisen välityshakemiston välille ensimmäisen tunnistuksen perusteella ja välineet yhteyden muodostamiseksi käyttäjän ja toisen välityshakemiston välille toisen tunnistuksen perusteella, jolloin ensimmäinen ja toinen tunnistus poikkeavat toisistaan tunnistuksen luotettavuuden (vahvuuden) perusteella.

(57) Tiivistelmä

Keksinnön kohteena on menetelmä ja laitteisto tiedonsiirron hallitsemiseksi tietoverkossa. Erityisesti keksintö koskee luottamuksellisen tiedon välittämistä tietoverkossa. Keksinnön eräänä ajatuksena on se, että kun käyttäjälle tarkoitettu tieto on tallennettu (413), tallennuspaikan osoite siirretään käyttäjälle luotettavan tahon (välittäjän, 440) välittämänä. Tällöin välittäjän suorittaman käyttäjän tunnistuksen perusteella käyttäjän on mahdollista saada käyttöönsä useiden tiedon/palvelun tuottajien tiedot/palvelut.

Fig. 4

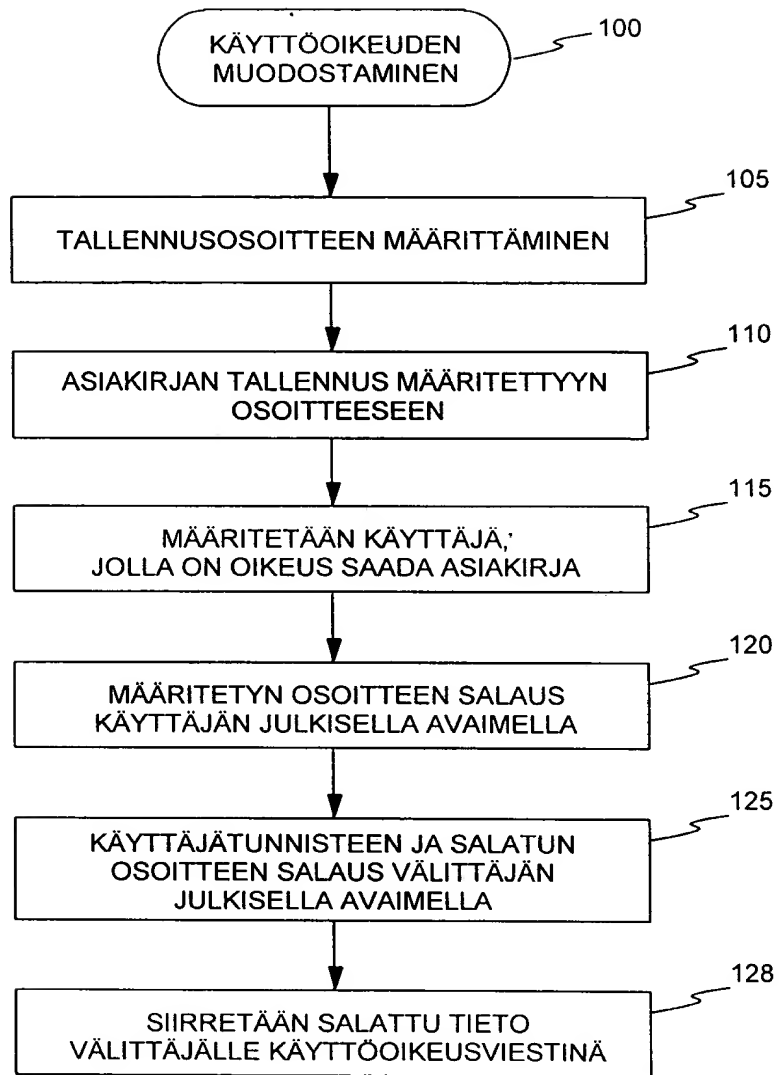


FIG. 1

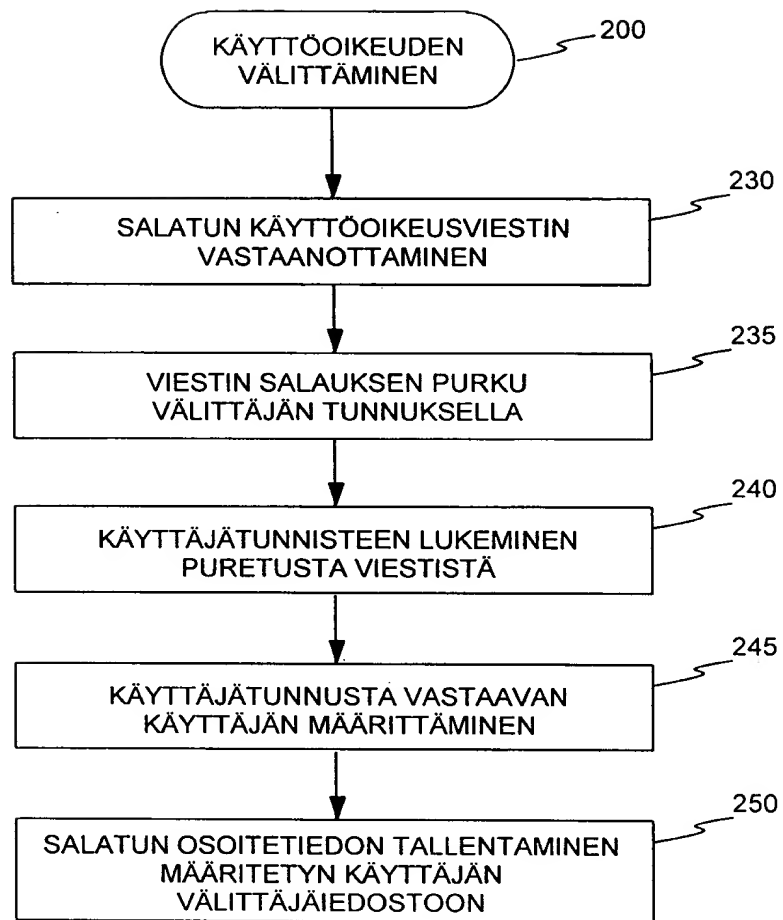


FIG. 2

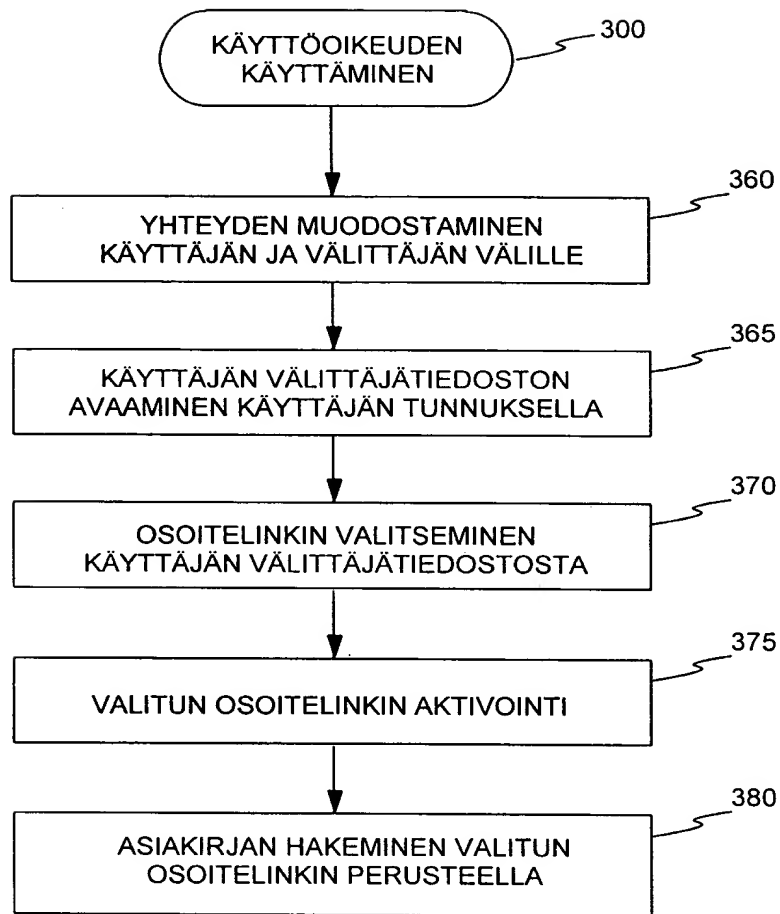


FIG. 3

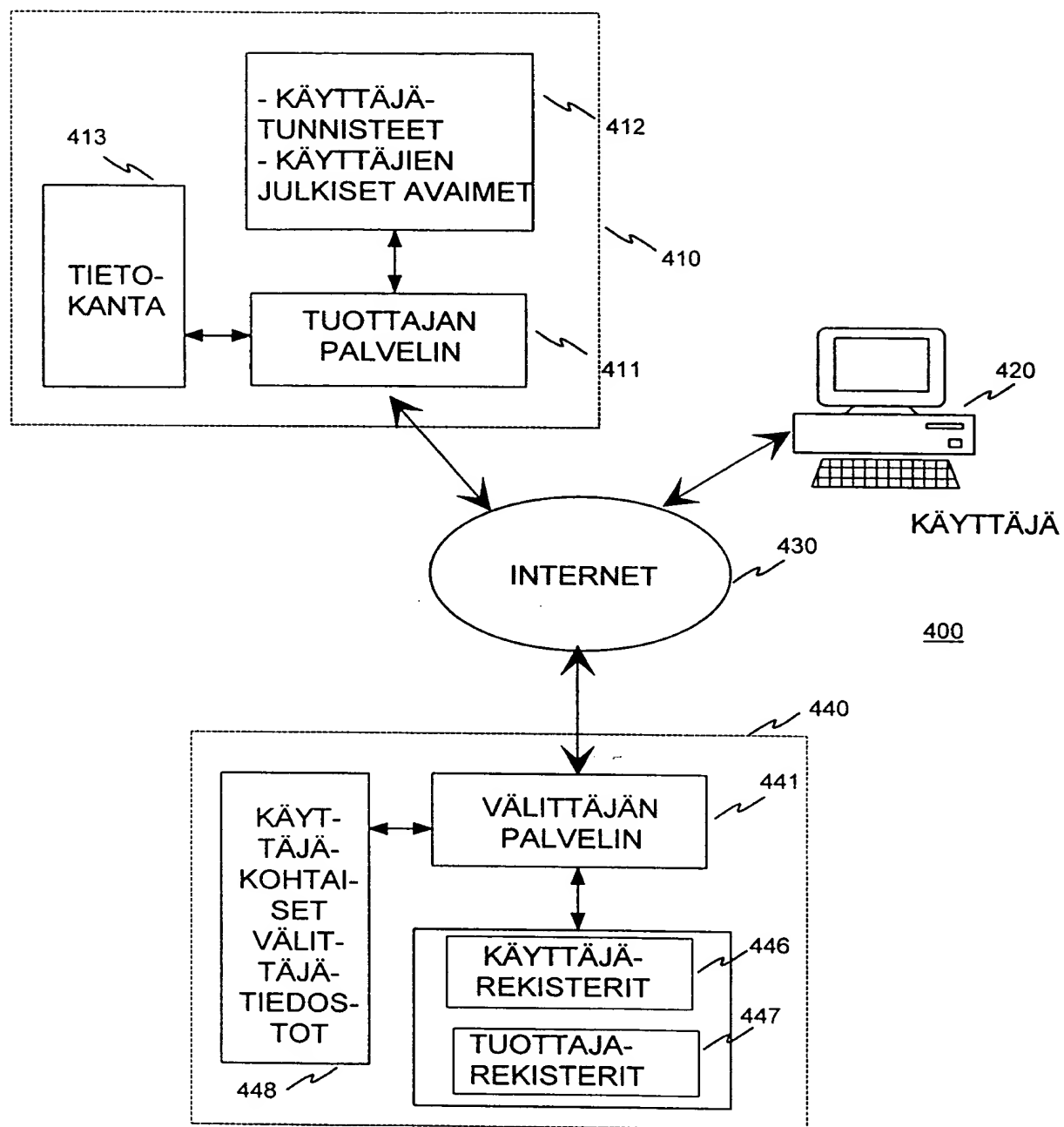


FIG. 4

50

VÄLITTÄJÄ: SUOMEN POSTI 51

VÄLITYSHAKEMISTO: Kaisa Käyttäjä 52

| LÄHETTÄJÄ 53 | AIHE 54 | LINKKI 55 | PVM. 56 |
|---------------------|-------------------|--|-----------|
| Verkkomedia Oy | Verkkolehti no. 6 | www.verkkol.fi/6 | 1.6.2000 |
| Net-Fly Ltd | Kanta-as.tiedote | www.fly.fi/abc | 20.5.2000 |
| Verkkomedia Oy | Verkkolehti no. 5 | www.verkkol.fi/5 | 1.5.2000 |
| H:gin kärkeäjoikeus | Haaste | www.ko.fi/123 | 15.4.2000 |

FIG. 5